

### **REMARKS**

Applicant respectfully requests reconsideration and allowance of the subject application.

#### **General**

Claims 1-14 are pending. Claims 1-9 and 11-13 have been amended in response to the Examiner's rejections. Claims 15-20 are new.

Support for new claims 15-20 is found in original claims 6-8.

Claim 6 has been amended to correct the statement that "said device is a standard credit card." The device claimed in claim 6 comprises the novel features of claim 1, and is not strictly "standard." The description in paragraph [0034] of a device that "can also work with existing magnetic swipe or Smart Card readers and with ATM machines" clearly supports a user device according to the invention that is "a card readable by a standard credit card reader" as now recited in claims 6 and 15.

No new matter has been added by this amendment.

#### **Allowable Subject Matter**

The Examiner has acknowledged that claim 14 is allowable. Additionally, the Examiner has acknowledged that claims 5-8 and 13 would be allowable if rewritten in independent form including the limitations of the base claim and any intervening claims. Claim 13 has been rewritten in independent form and is therefore deemed now to be allowable. Applicant appreciates the indication of allowability.

#### **35 U.S.C. §103(a) Claim Rejections**

Claims 1, 2, 9, and 10 have been rejected under 35 U.S.C. §103(a) as being unpatentable over European Patent Application No. 1 041 523 A2 (Baird) in view of International Publication No. WO 01/75826 (Maguire) and further in view of U.S. published Patent Application No. 2001/0018660 (Sehr), which the examiner alleges to show "old and well known" features. With respect to the amended claims, applicant respectfully traverses this rejection.

Baird shows a self-service terminal such as an automatic teller machine (ATM). The ATM includes a biometric sensor, which the examiner points out may be a fingerprint reader. The read biometric data are sent to a remotely located third-party user identifying unit (30) where they are compared against stored data. Once the biometric data are approved as valid, the user identifying unit authorizes a transaction. The manner of transmitting the authorization is not explained. The user identifying unit 30 produces a random code as a "transaction identifier." The random code is recorded in the memory of the user identifying unit, and sent to the ATM, to be used in the event of a dispute to match the ATM's transaction record to the user identification unit's record of the biometric. At the time of transaction, the random code does not and cannot act as a Personal Identification Number, because the receiving ATM has nothing to compare it against.

Maguire is cited as disclosing generating a pseudo-random PIN. However, Maguire discloses only generating a PIN before a card is issued.

Sehr is cited as disclosing a smart card that may contain fingerprint or other biometric data. However, Sehr's smart card only passively contains imprinted data. The biometrics box (13) that scans the fingerprint, and the processor that compares the scanned and stored fingerprints, are parts of the larger system.

In both Baird's and Sehr's systems, the authentication of the fingerprint or other biometric data is conducted in the network and, once the user's identity is authenticated, permission to proceed with the transaction is passed over the network.

In the present invention, in contrast, the fingerprint authentication takes place entirely on the smart card or other user device. Because the card is not connected to the network, the permission to proceed cannot be transmitted over the network. Therefore, when the card is activated by the user, and when the card confirms that the user physically holding the card is the rightful owner of the card whose fingerprint is stored on the card, the card generates a PIN that the user can use to authenticate a transaction. The present invention is an improvement over

systems such as Baird's and Sehr's because it does not require bulky, expensive and vulnerable biometric scanners at every ATM or other point of sale. The card itself is more sophisticated and more expensive, but the card usually remains in the possession of the owner, who has an incentive to take care of his or her card. The present invention is an improvement over conventional credit card and smart card systems, because the PIN is used only once, and a new PIN can be generated only by the owner. The present invention is exceptionally simple to use, because the fingerprint scanner can be placed on the card in a position where the user will naturally hold the card. The user thus merely has to hold the card and read the PIN off the display. There is no disclosure or suggestion in any of the cited references of a smart card or other device in accordance with the present invention, and the present invention, as claimed in claims 1 and 9, is believed to be non-obvious over the cited references.

It is not clear that in the rejection of claims 1 and 9 the examiner has given proper weight to the requirement of the claims that the reader, memory, comparator, and pseudo-random generator are on the user device. In order to ensure that these features are given proper weight, claims 1 and 9 have been amended to specify that the device claimed in claim 1, and used for the method of claim 1, is a "user device" (basis for which is found in paragraphs [0008] and [0033]), and to reiterate in reciting each of the reader, memory, comparator, and pseudo-random generator that these elements are on the user device. There is no disclosure or suggestion in the cited prior art of providing these elements on the user device. It would not have been possible in the prior art to provide these elements on the user device, because the cited prior art all relies implicitly on a secure network connection from the biometric comparator to the ATM or other controlled system.

In addition, the examiner's motivation for combining Baird and Maguire is traversed. As noted above, Baird does not use a PIN. Baird uses a random number solely as a unique identifier for later matching of records. The examiner argues that "it would have been obvious ... to modify the device disclosed by Baird to include a pseudo-random PIN ... because it provides an additional level of security making it [difficult] for pirates to determine the PIN." The examiner's argument does not apply to Baird's disclosure. There is nothing in Maguire that would have motivated a person of ordinary skill to replace Baird's random unique identifier, and

there is nothing in Maguire that would have motivated a person of ordinary skill to introduce a PIN to Baird's system. For these reasons also, the present invention is deemed non-obvious over the cited prior art.

All remaining pending rejected claims depend from either claim 1 or claim 9, and thus are allowable for at least the same reasons as set forth with respect to claims 1 and 9.

In addition, however, claims 2 and 10 recite that the pseudo-random generator generates the PIN in accordance with a user specific algorithm. The examiner asserts that feature is disclosed at page 6, lines 13-19 of Maguire, but no such disclosure can be found. In fact, in Maguire's system at its most restrictive, the algorithm is specific to the card issuer. In the present invention as claimed in claim 2, the algorithm is specific to the card user.

Claims 3 and 11 recite the card further comprising a display for displaying the PIN. The examiner cites the PIN pad mentioned in paragraph [0061] of Sehr, but a conventional PIN pad like Sehr's never displays the PIN. The examiner's argument that "it would have been obvious ... to include a display for displaying said PIN ... because it prevents unauthorized user from accessing the information" is not credible. It is exactly to prevent unauthorized persons from accessing a PIN that PIN pads do not display the PIN. In any case, the examiner has overlooked the requirement, which claims 3 and 11 have been amended to point out more specifically, that the display is on the user device. It is only after the user has read the one-use PIN off the display on the smart card or other user device that the user inputs the PIN into, for example, a PIN pad like Sehr's, from which the PIN is "forwarded to an issuer of said device which grants access to said information."

For these reasons also, the present invention, as claimed in claims 2, 3, 10, and 11, is deemed non-obvious over the cited references.

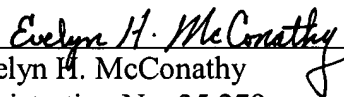
### **Conclusion**

In view of the foregoing amendments and remarks, all pending claims are in condition for allowance. Applicant respectfully requests reconsideration and issuance of the pending claims. If

any issues remain that preclude issuance of this application, the Examiner is urged to contact the undersigned attorney.

Respectfully submitted,

Date: June 2, 2006

  
Evelyn H. McConathy  
Registration No. 35,279  
DRINKER BIDDLE & REATH LLP  
One Logan Square  
18<sup>th</sup> and Cherry Streets  
Philadelphia, PA 19103-6996  
Tel: (215) 988-3361  
Fax: (215) 988-2757